

# Making Intrusion Event Analysis easy

June 3rd, 2009



ENTERPRISE THREAT MANAGEMENT

### Agenda

- Adaptive IPS Today
- Adaptive IPS with RNA
- Competitive Comparisons
- Adaptive IPS Benefits







# Adaptive IPS In-Depth





# What is Adaptive IPS?

- Strategy for making the IPS:
  - Contextual
  - Self-tuning
  - Performance-efficient
  - More accurate and non-evadable
- Leverages network intelligence provided by RNA
- Benefits:
  - See only what's relevant
  - Handle more traffic faster
  - Put less effort into tuning
  - Avoid security evasions and detect traffic more accurately



# Adaptive IPS Components

- 1. Impact Analysis
- 2. Automated IPS Tuning
- 3. Adaptive Traffic Profiles
- 4. Non-Standard Port Handling





# 1. Impact Analysis



#### We know what this is! Impact Flags!

Impact Flag Rating	Target Network Monitored by RNA	Target Host Monitored by RNA	Exploit Matches Target OS and/or Service	Exploit Targets a Known Vulnerability
1	Yes	Yes	Yes	Yes
2	Yes	Yes	Yes	No
3	Yes	Yes	No	No
4	Yes	No	Unknown	Unknown
0	No	No	Unknown	Unknown

- Impact Flag 1 Act immediately!
- Impact Flag 2 Investigate
- Impact Flags 3, 4 & 0 Good to know



# 2. Automated IPS Tuning

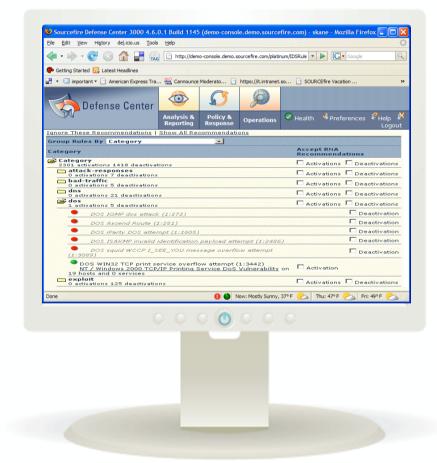
- We know this one, too!
- RNA Recommended Rules
  - RNA recommends Snort rules to enable based on the assets you're protecting
  - Maximizes network protection
  - Maximizes 3D Sensor resources





### Let's See a Demo!







# 3. Adaptive Traffic Profiles

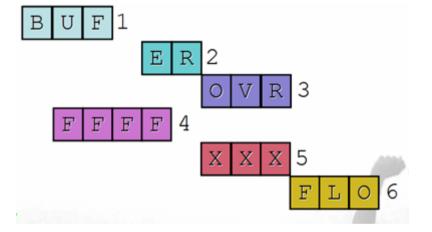


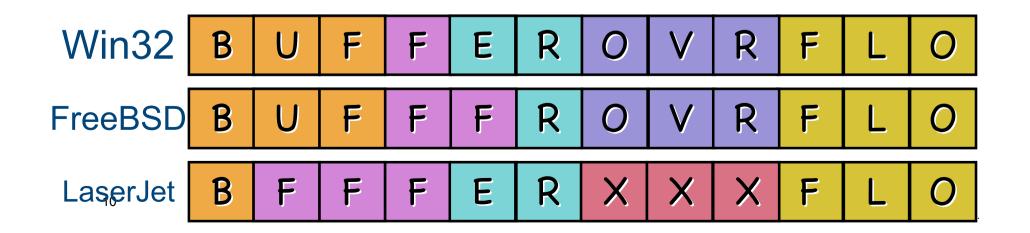
- Uses RNA network intelligence about the target host's operating system
- Models traffic the way that operating system would see it
- Other IPS products need to make assumptions about how to model traffic that are often wrong
- Avoids evasions



# 3. Adaptive Traffic Profiles, cont.

- Different operating systems sometimes "see" the same traffic differently
- If IPS and target see traffic differently, this can cause evasions
- Danger: IPS misses the attack but the target sees it





### 4. Non-Standard Port Handling



- IPS automatically applies appropriate rules to traffic on nonstandard ports
- If HTTP is running on port 8080, RNA knows this. The Defense Center will instruct the IPS to apply HTTP rules to port 8080.
- Benefits:
  - Reduced manual administrator tuning
  - Maximized network protection



# Adaptive IPS – Industry Comparison



Capability	SOURCE fire*	TippingPoint	INTERNET SECURITY SYSTEMS	<b>NcAfee</b>	cisco	
Impact Analysis	1		Limited	Limited		
Automated IPS Tuning	1					
Adaptive Traffic Profiles	1					
Non-Standard Port Handling	1		>	Limited		

# Summary of Benefits

- Maximizes network protection
- Maximizes IPS performance
- Minimizes the quantity of actionable events
- Minimizes the need for manual IPS tuning
- Minimizes false positives
- Minimizes network security risks





# Adaptive IPS Technology Brief

#### Available now!

http://www.sourcefire.com/resources/downloads/public/techbrief/SF\_T B\_AdaptiveIPS.pdf

TECHNOLOGYBRIEF  TECHNOLOGYBRIEF  Sourcefire Adaptive IPS  data transmission  point of the avortable  data transmission  point of the avortable  data transmission  d	CHCHNOLOGYURIES out introducing "noise" or false positives, out blocking lagitmate traffic, and without with the second second second second second second second second second second second without the second second second second pactive, RNA Recommanded Pulses into how mean as set of IPS rules for a user's out an environment. From a functional mean second second second second second pactive, RNA Recommanded Pulses into how mean as set of IPS rules for a user's out an environment. From a functional mean second second second second second second second second second second lad network. The result is a set of momend utions that rules to a storad momend second second second second second second second second s	Litably crafted threat will be reparcy. The IPS Evasion is by eliminating the quation. This is mically adjusting the at a 3D Sensor uses for any inspire of the destination figure exceptions is also personing the feature for nating that corresponding sembled in a particular way. andling. The relationship es and port is based on seludes the use of non- ning HTP on TCP 800 will go of non-standard ports butty reactions. Alternately, er-centric applications (e.g., en use non-standard ports butch applications (e.g., en use non-standard ports and port handling capability for such scenarios. This is incluly applying the outs and services for the net result is that ave to manually configure where services are running	<ul> <li>THE BENEFITS OF ADAPTIVE IPS</li> <li>Organizations can derive the following benefits</li> <li><b>0. Sparting and efficiency is improved.</b> Whether semi-sustmatic of thy dynamic, the turing option afforded by Adapter IPS can be adapted by the semi-submatic of the PS can be adapted by the semi-submatic of the PS can be adapted by the semi-submatic of the semi-subject to confinue to the semi-subject of the semi-subject to confinue to the semi-subject of the semi-subject to confinue to the semi-subject of the semi-subject of semi</li></ul>
Security for the real world. MANAGEMENT with mass real real real real real real real real	out introducing "noise" or false positives, out blocking legitimate traffic, and without ing critical attacks. Reacommended Rules. The RNA- service attacks and the service service and the minimal as led TIS rules for a user's oular environment. From a functional peotive, RNA-Reacommended Rules involves a steps. First, RNA establishes a profile for a in network, identifying al hosts, the operating peotive, RNA-Reacommended Rules involves are using to communicate, and the enablines to which they are potentially applible. Next, this inventory is compared to fuels and the reacommender and the are using to communicate, and the enablines to which they are potentially applible. Next, this inventory is compared to fuels and the releast. For example, a le indicating the presence of Linux-based s would result in the recommendiation to added unived from the rulesest. For example, a le indicating the presence of Linux-based s would result for a lained hyse some for inistrators can choose to accept the mineradations wholesale or modify them as	It by eliminating the quation. This is incluib adjusting the input the this is not not not not the destination figure exceptions is also appressing the feature for noting the corresponding sembled in a particular way. and filing. The relationship schudes the use of non- nning HTP on TCP 8060 act, some organizations will ge of non-standard ports builty reasons. Alternating, on use non-standard ports builty reasons. Alternating, on use non-standard ports and schudes the actual result as a schule the partities the actual the particular the part of the schule the part for such schule the part of the schule the pa	Organizations can derive the following benefits from Adaptive IPS: • Operational efficiency is improved. Whether emi-automatic of fully dynamic, the uning uspriticative reduces the effort regulard to establish and maintain ideal configurations for IPS sensor, sepecially in computing environments that are subject to configurations for each of the establish and maintain ideal configurations escuring analytic to scattering and environments that are subject to configuration of security advectory and subjects to spend cycles tackling other challenges, such as securing a new Volf inglesematism or compliance requirements. • Security effectives is ingreened Adjusting packet processing techniques, inspection rules, and other aspects of sensor configuration to correspond to the relevant characteristics of the actual systems that are being proteined is negatives, thereby enabling security administrations of derived and in fully dynamic manner only serves to multiply the solvantage. • Systems performance is improved. Both individual sensors and the Defense Center mansgement infrastructure benefits on the elimination of upmecessary rules and the corresponding dramits.
Security for the real world. MANAGEMENT With TESS Particular and the real world. MANAGEMENT MANA	out blocking logitimate traffic, and without ing ortical attacks. <b>Hecommended Rules</b> . The RNA- mmendad Rules feature leverages the power NA (Real-time Natwork Awareness) to minend a set of 16P rules for a user's cular environment. From a functional observed the set of the set of the set of the stress First, RNA establishes a profile for a n network, identifying all hosts, the operating sms and services they are running, the ports are using to communicate, and the setbilines to which they are potentially aptible. Next, this investory is compared to tue not for RT result is a set offer the mendations for rules that should be added mmendation to the recommendation to add sing" Lunux-criented rules to a sensor particular to approximate the source source the sensor the sensor the sensor source source the sensor the recommendation to add the prosensor the sensor the provide the source the recommendation to add the sensor the sensor	h input from RNA that isystem of the destination figure exceptions is also represent the destination figure exceptions is also nating that corresponding sembled in a particular way. and ling. The relationship es and ports is based on ecludes the use of non- ning HTTP on TCP 808 will ge of non-standard ports builty reasons. Alternately, encontra capications (e.g., en use non-standard ports builty reasons. Alternately, encentra capications (e.g., en use non-standard ports builty reasons. This is nically applying the given session based on antifies the actual ort result is visual we to manually configure where services are running	<ul> <li>options afforded by Adaptive IPS can be set and the information of the set of t</li></ul>
to increasingly look for more utions. Many IT security of PRINE genese of Affeion-y used to achieve aprivation of threats to their resources continue to systet and private and the security estimation of threats of the security and the security and the security of the security of the security and the security of the security of the security and the security of the security of the security of the security of the security of the security of the security and the security of the security of the security of the security and the security of the se	ammended Rules feature leverages the power NA (Real-time Network Awareness) to immend a set of IPS rules for a user's proteine RNA-Recommended Rules involves steps. First, RNA establishes a profile for a network, idontrying all hosts, the oparating profile RNA establishes a profile for a network idontrying all hosts, the oparating and a services they are running, the ports are rules and the running of the profile profile RNA, this inventory is compared to rule set for the IPS sensoridy protecting the led network. The result is a set of mineradiation for rules that should be added be indicating the presence of Linax-based is would result in the recommendation to add signation that define to a allow some for instrators can choose to accept the mineradiations tholesale or modify them as	sembled in a particular way. andling. The relationship es and ports is based on ecludes the use of non- ning HTTP on TCP 808 will be an explored to the semi- relation of the semi- econtric andhard ports with reasons. Alternately, en use non-standard ports and port handling capability for such scenarios. This is nically applying the given session based on antifies the actual of the actual of the actual of the actual of the actual of the set of the actual of the actual of the set of the actual of the actual of the set of the actual of the actual of the actual the actual of the actual of the actual of the actual the actual of the actual of the actual of the actual the actual of the actual of the actual of the actual of the actual the actual of the actual the actual of the actual the a	change. This also has the side benefit of freeing security administrators and analysta to spend security administrators and analysta to spend security a new VoIP implementation or addressing the ever-growing population of compliance requirements. Security affectiveness is inspreved. Adjusting packet processing techniques, inspecto nulse, and other angetto of senor configuration to the security affectiveness is inspreved. Adjusting packet processing techniques, inspecto nulse, and other angetto of senor configuration to the estable spread of the second security addination administrators to identify and respond mored emusing that attacks are properly blocked. Making these adjustments in a fully dynamic manner only serves to multiply the advantage. System performance is impreved. Both individual sensors and the Defense Center management infrastructure benefits from the elimination of or events that they would inevitably generate.
TECHNOLOGYBRIEF TechnologyBRIEF Sourcefire Adaptive IPS are a private and the accurate of the	is steps. First, RNA establishes a profile for a n network, identifying all hosts, the oparating amis and services they are running, the potst and the services of the service and the service profile and the service and the service application back the service leaf network. The result is a set of mmendations for rules that should be added mmendations for rules that should be added in the service service should result the recommendation to add sing". Linux-chanted rules to a sensor diguaration that define the account inistrators can choose to account the mmendations tholesale or moder the mendations wholesale or moder the me	act, some organizations will ge of non-standard ports putry reasons. Alternately, encornic applications (e.g., en use non-transferd ports red port handling capability for such scenarios. This is nically applying the given session based on artifies the actual port fresult is that the services are running	<ul> <li>Sacurity effectiveness is improved. Adjusting packat processing tachniques, inspection rules, and other aspects of sensor configuration to correspond to the relevant characteristics of the actual systems that are being protected is certain to rule close false positives and false administrators to identify and respond more quickly to those events that matter most, and ensuring that attacks are properly blocked. Making these adjustments in a fully dynamic manner only serves to multiply the advantage.</li> <li>Systems performance is improved. Both individual sensors and the Defense Senter management in most provide and the corresponding stream of events that they would inevitably generate.</li> </ul>
the r origination dispute of user profile are to individual ensures profile set to individual ensures profile to resource of the resources able IT resources. profile to resource of the resources profile to resource of the resources to resource of the res	paptible. Next, this inventory is compared to uius set for the JPS sensoridy protecting the leaf network. The result is a set of moved from this relatest. For exempts added is indicating the presence of Linaz-based is undicating the presence of Linaz-based s would result in the recommendation to added using" Linux-oriented rules to a sensor fuguration that def not already have some for inistrators can choose to accept the mmendations wholesale or modify them as	rid port handling capability for such scenarios. This is nically applying the given session based on entifies the actual orts and services for the net result is that save to manually configure where services are running	certain for reduce false positives and false megative. There by enabling accurby quickly to those events that matter montor quickly to those events that matter montor ensuring that tatles are properly blocked. Making these adjustments in a fully dynamice. System performance is improved. Both individual sensors and the Defense Center ransgement infrastructure benefit from the elimination of urnecessary rules and the corresponding stream of events that they vouid intrability generates.
Sourcefire Adaptive IPS resources re	s would result in the recommendation to add sing" Linux-oriented rules to a sensor iguration that did not already have some (or of them in place. Finally, security inistrators can choose to accept the mmendations wholesale or modify them as	entifies the actual orts and services for the net result is that have to manually configure where services are running	manner only server to multiply the sidvantage. Systam performance is improved. Both individual sensors and the Defense Center management infrastructure benefit from the elimination of unnecessary rules and the corresponding stream of events bits they would invitably generate.
hiss of their security income epicyment of a network desis ystem (IPS), Historically, of a come or network-bene thread and spatial of network-bene threads, it is the "noise" it creates and of network-bene threads, it fuelt "noise" it creates and of network-bene threads and of network-bene threads and of network-bene threads and of network-bene threads of the security and the security auto auto	mmendations wholesale or modify them as		, ,,,
Initiat is being profilered, initiat is being profilered, minitiation spriced in under the profilered profilered in the profilered profilered into a set of the profilered profilered with the profilered profilered profilered to a set of the profilered profilered profilered profilered profilered profilered profilered into a set of the profilered profil	red. To aid this step, recommended rules are evientiv organized by category of e.g., coerating any, service, threat type), and can be selected preservice, threat type), and can be selected preservice, the selected selected preservice and the selected selected trigg in the future. A second the selected selected population of the selected selected population of the selected selected population of the selected plate control of whether, and to a certain the differently Unfortunately, this provides the selected provides that advantage of a nique known as evaluant. The selected paragrade heat, for example, if the target host targeted heat. For example, if the target host selected paragrad heat for the same manner as	any measurement and monigence in a	Enably, Adaptive IPS is an integral part of the Sourcefit a Dystem. The same infrastructure that are associated with a complete Enterprise That are associated with a complete Enterprise operational perspective. Enterprise Thread Management, of the Sourcefire by System, visit Sourcefire's web site a two sourcefire.com or contact Sourcefire today. The "Bacescale stated basics are seen above the total to solve and the source and the source of the total source and the source of the source of the total source and the source of the source of the source of the source of the source of the source of the total source of the source of the source of the total source of the source of the source of the source of the source of the source of the source of the source of the source of the source of the source of the total source of the source of t
	SOURCE fire 2		SOURC

# **Questions?**





